FortiAuthenticator - Certificate Based SSL VPN Solution Guide

VERSION 1.0

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

09/10/2015

FortiAuthenticator 4.0 - Certificate Based SSL VPN Solution Guide

23-330-264235-20150901

TABLE OF CONTENTS

Change Log

Date	Change Description
2013-10-23	Initial revision

Introduction

This document provides a configuration guide for setting up certificate based SSL-VPNs using FortiGate and FortiAuthenticator. The guide provides a step by step walkthrough on both the FortiAuthenticator and the FortiGate, however, for a detailed understanding on PKI and certificate authentication further reading is required, as the objective of this guide is to provide a configuration walkthrough.

Software Versions

The configuration discussed in this document was tested on the following firmware versions:

- FortiAuthenticator 3.0
- FortiOS 5.0 GA Patch Release 4

FortiAuthenticator Certificate Based SSL VPN Guide

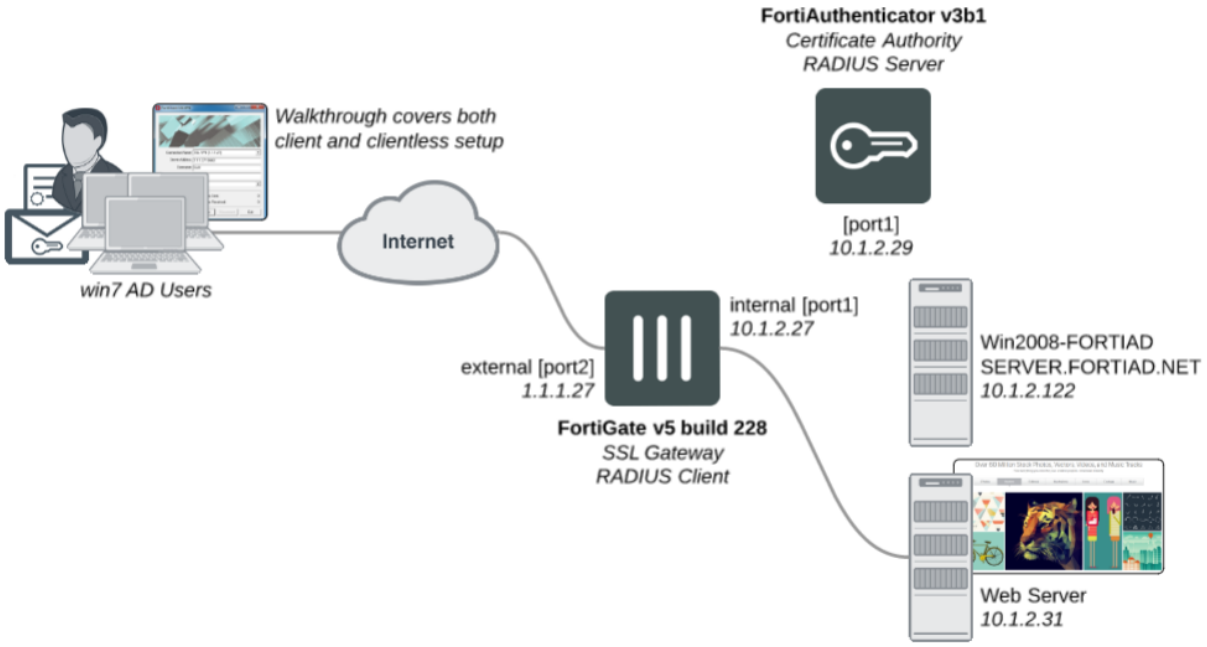
Introduction

The purpose of this document is to provide a configuration guide on how to setup certificate based SSL-VPNs, using FortiGate and FortiAuthenticator. The guide covers various subject areas such as PKI and VPNs, further reading is required for a detailed understanding on the theory of such topics, the intention of this document is to provide a concise configuration guide which will allow for the successful configuration of certificate based VPNs.

The guide will step through the FortiAuthenticator configuration before moving on the FortiGate, before testing the setup. All the topology components are using factory default settings, except for the IP configuration.

Before commencing the configuration, please ensure that the date and time are correctly configured and synchronized across all of the topology elements.

Topology

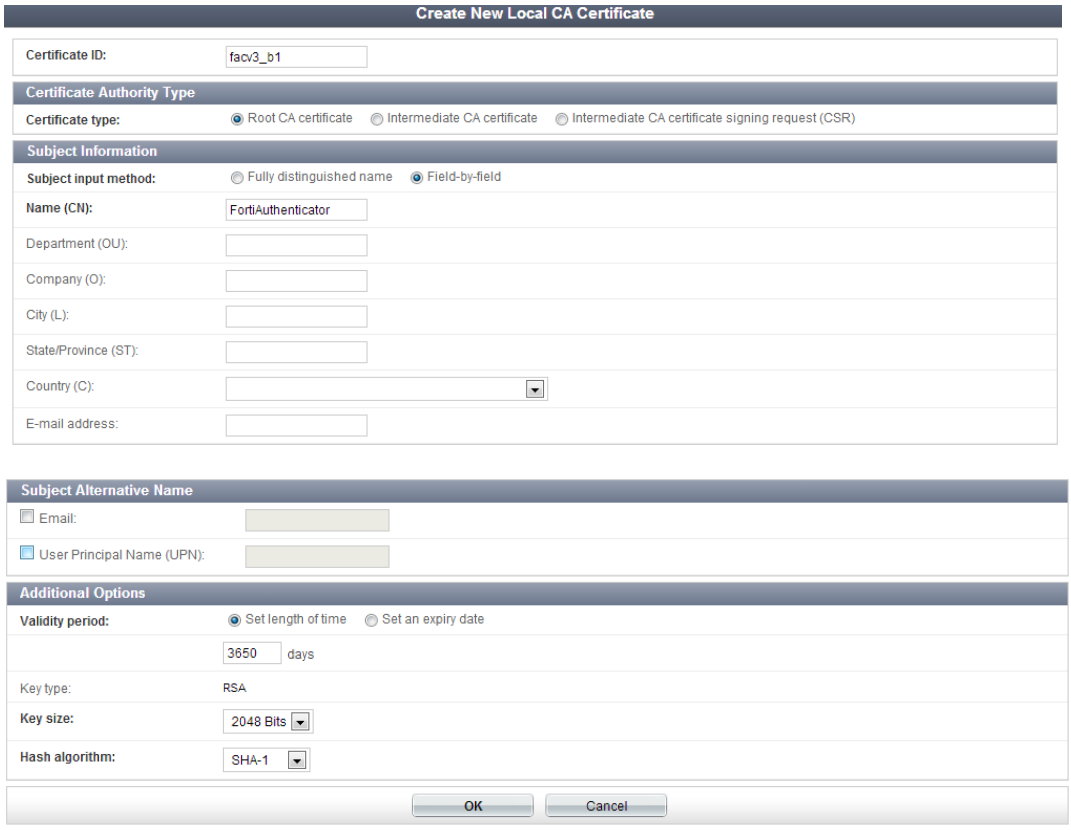


FortiAuthenticator Root Certificate

To commence the certificate setup on the FortiAuthenticator, a Certificate Authority root certificate has to be created (the FortiAuthenticator is the Certificate Authority in this configuration).

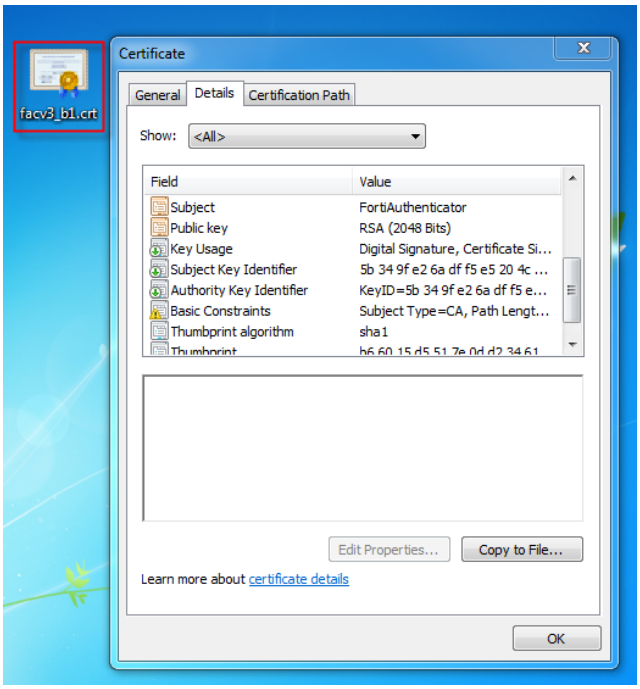
Under *Certificate Management* > *Certificate Authoritites* > *Local CAs* click *Create New*.

Complete the relevant certificate, example below and OK the changes.



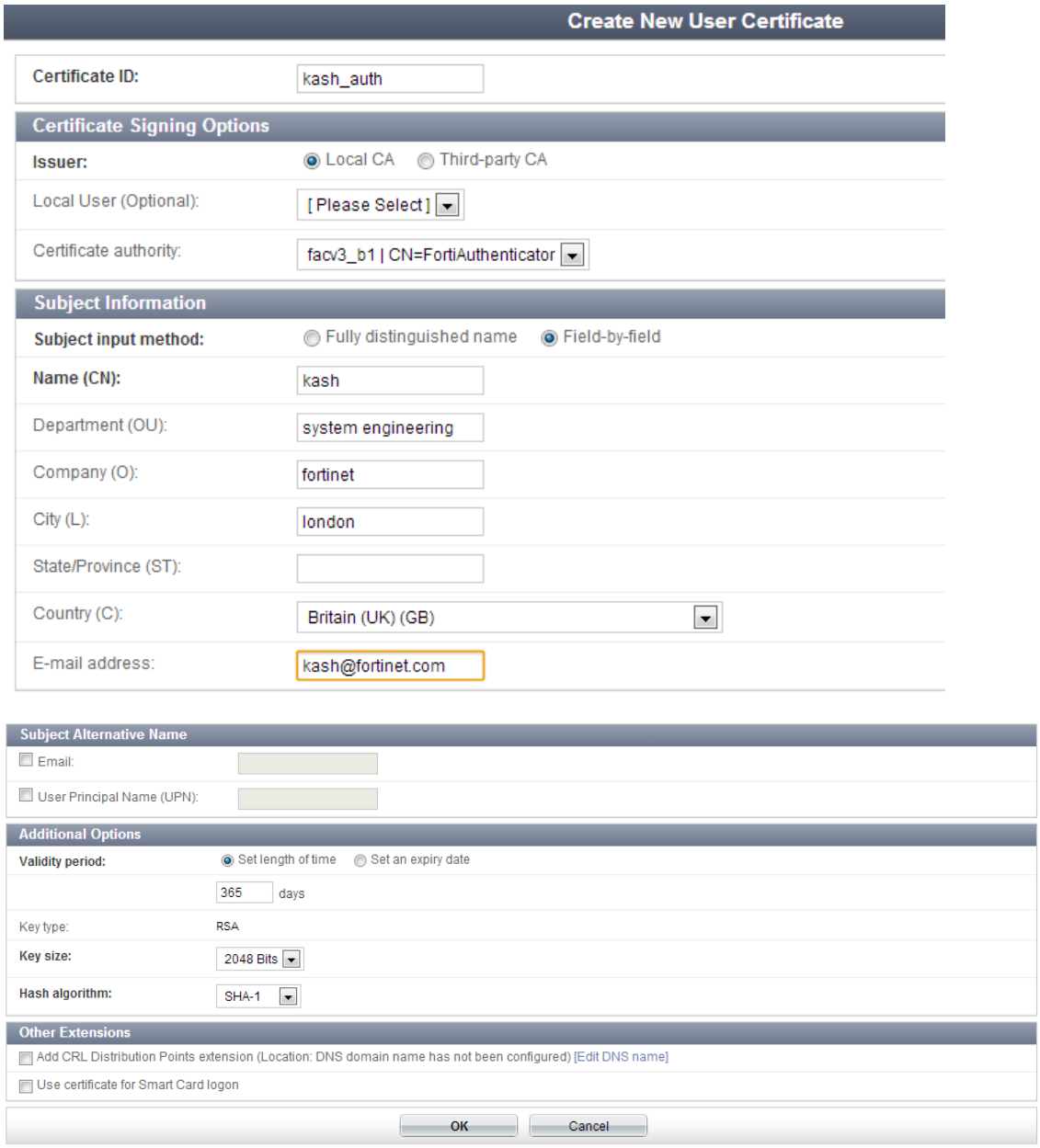
Once the certificate has been created, select the certificate and then click on *Export*.

Save the certificate to the desktop (or appropriate folder). Once the certificate is saved, it should be possible to double click on the certificate to view the details, see below.

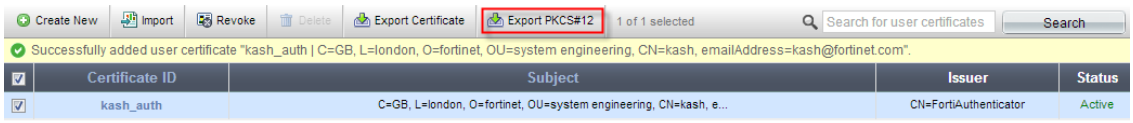


FortiAuthenticator User Certificate

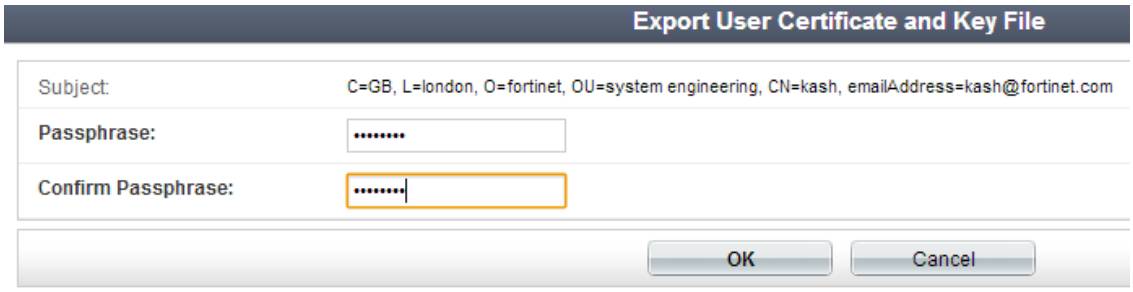
The next certificate based task is to create the user certificate. Within the FortiAuthenticator interface, go to *Certificate Management* > *End Entities* > *Users* and click on *Create New*. Then complete the relevant user certificate fields and click on *OK*, example below.



Once the certificate has been completed and OK'd, then export the certificate with the private key by selecting the certificate and clicking on *Export PKCS12#* button.

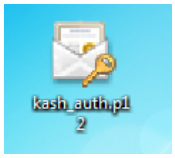


Add a *Passphrase* to the certificate being exported and click *OK*.

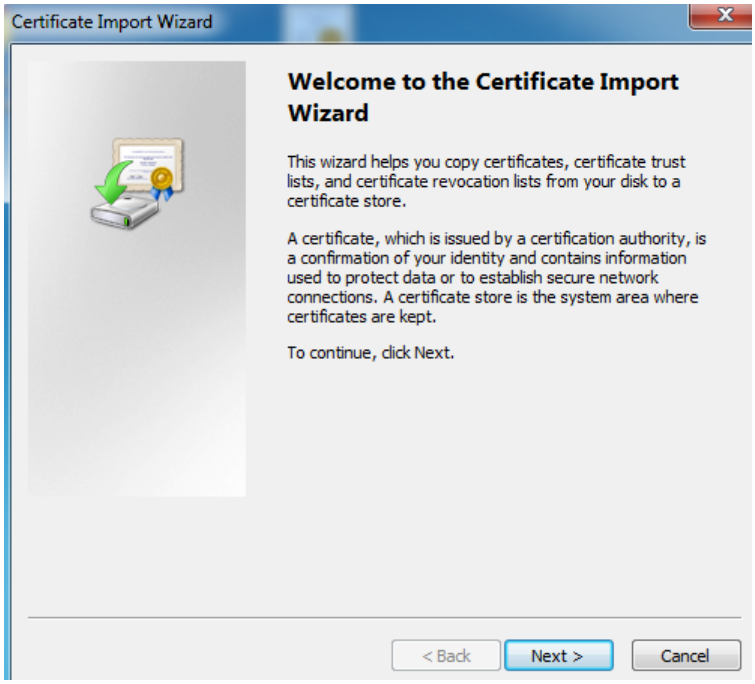


Then download the file to the desktop (or appropriate folder) by clicking *Finish*.

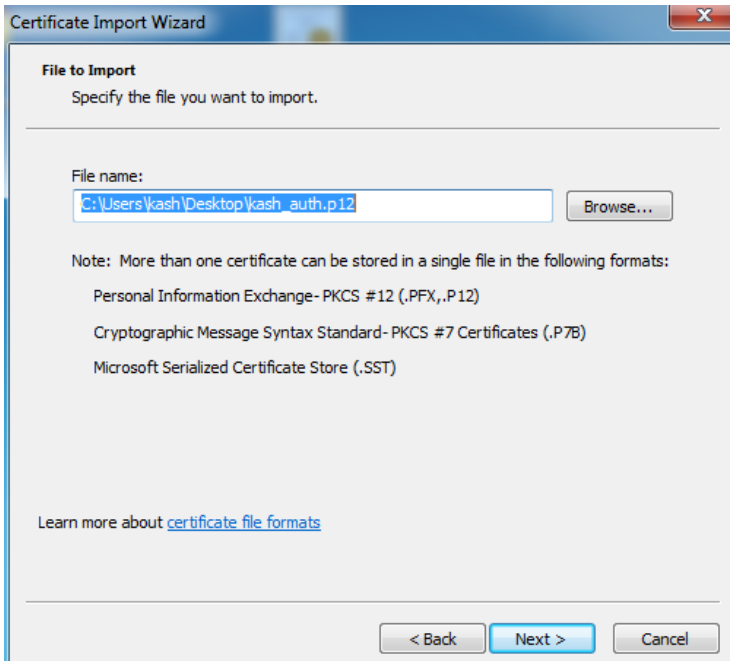
The PKCS12# file should be in the following format on the desktop:



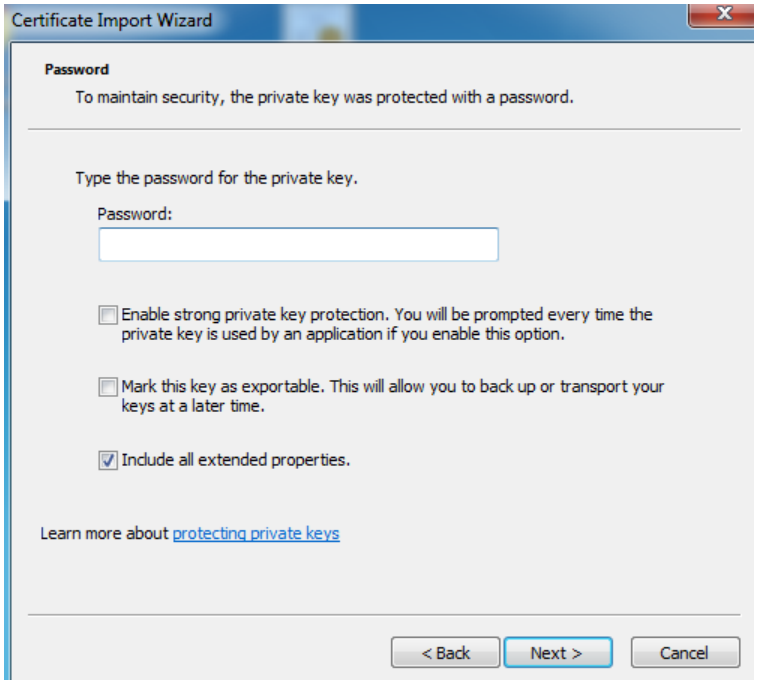
Double click the PKCS12# file, this should then start an automatic import wizard, see below. On the Welcome screen, click *Next*.



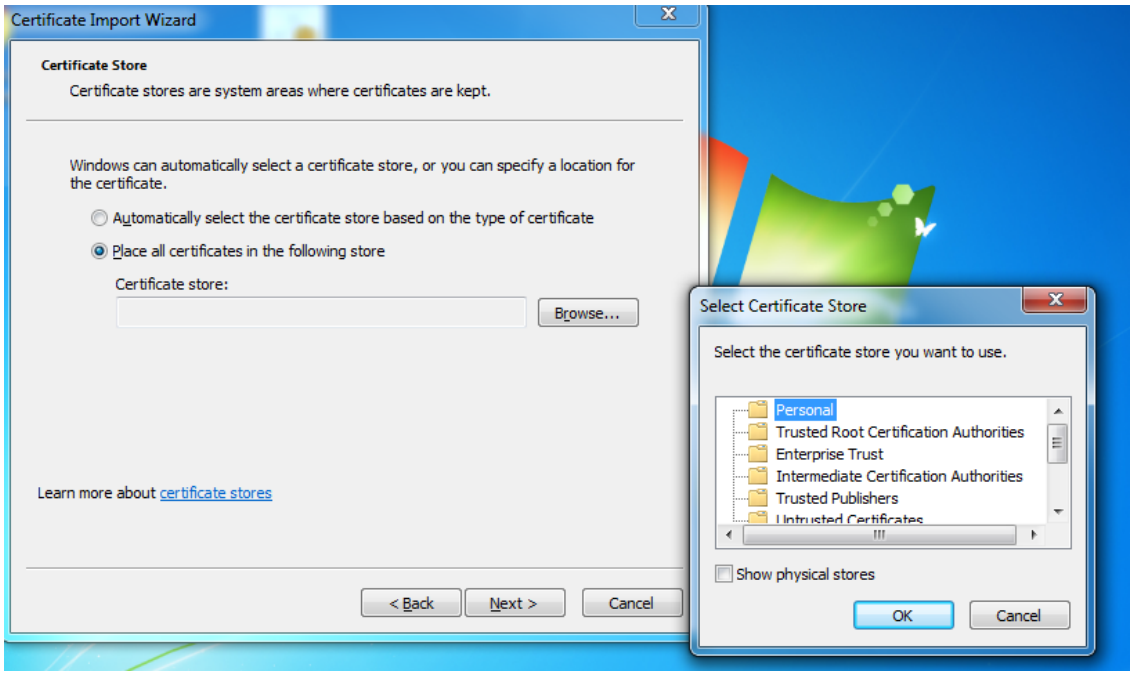
Ensure that the correct PKCS12# file is selected and click *Next*.



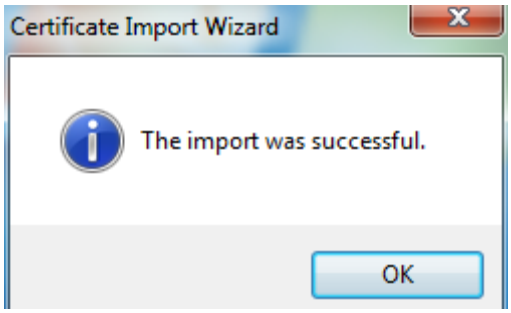
Enter the passphrase used during the export from the FortiAuthenticator and click *Next*.



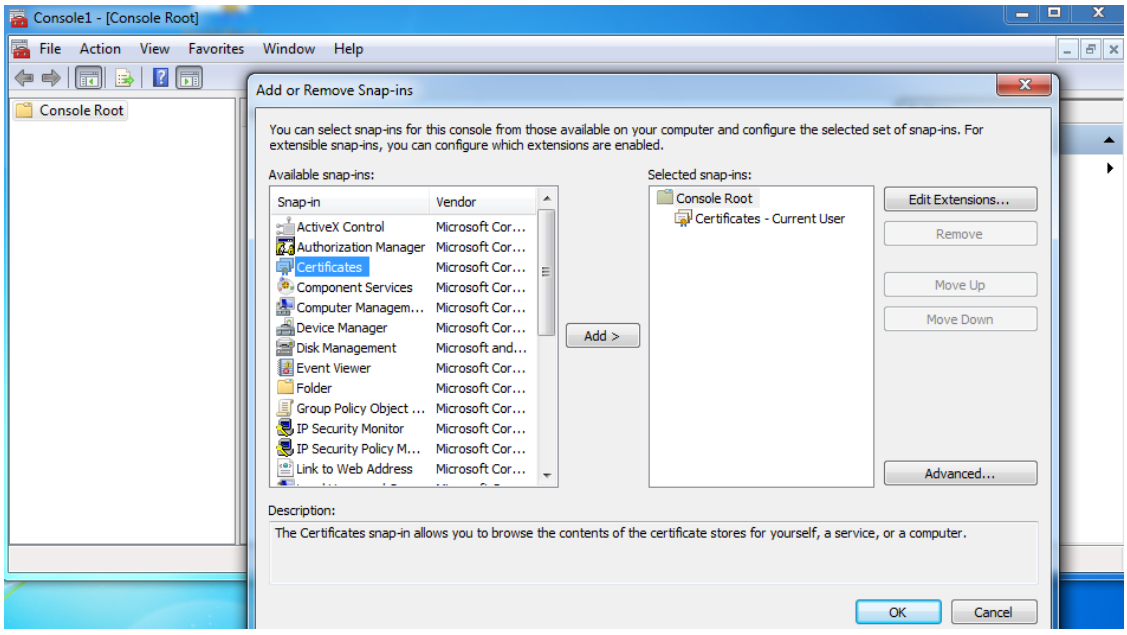
Ensure that the user certificate is being placed in the personal folder and click on *OK*.



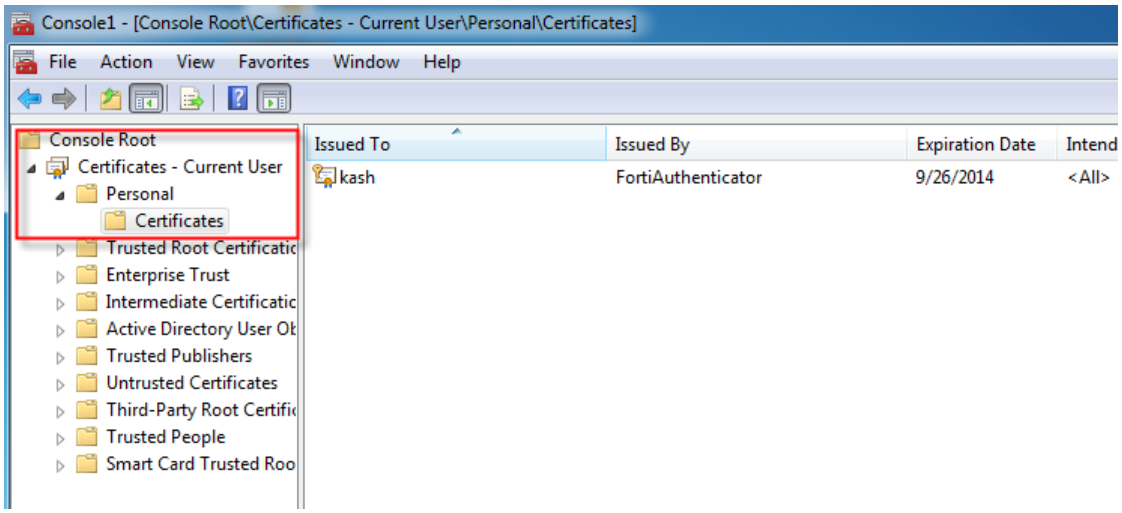
This should complete the user certificate import process and the following prompt should appear:



However, it is important to ensure that the certificate has been imported correctly and into the appropriate certificate store. To confirm the procedure, click on the Windows icon and type *mmc*, then press *Enter*. Then click on *File* > *Add/Remove Snap-In* and select the *Certificates* snap-in, as shown below, then press *OK*.



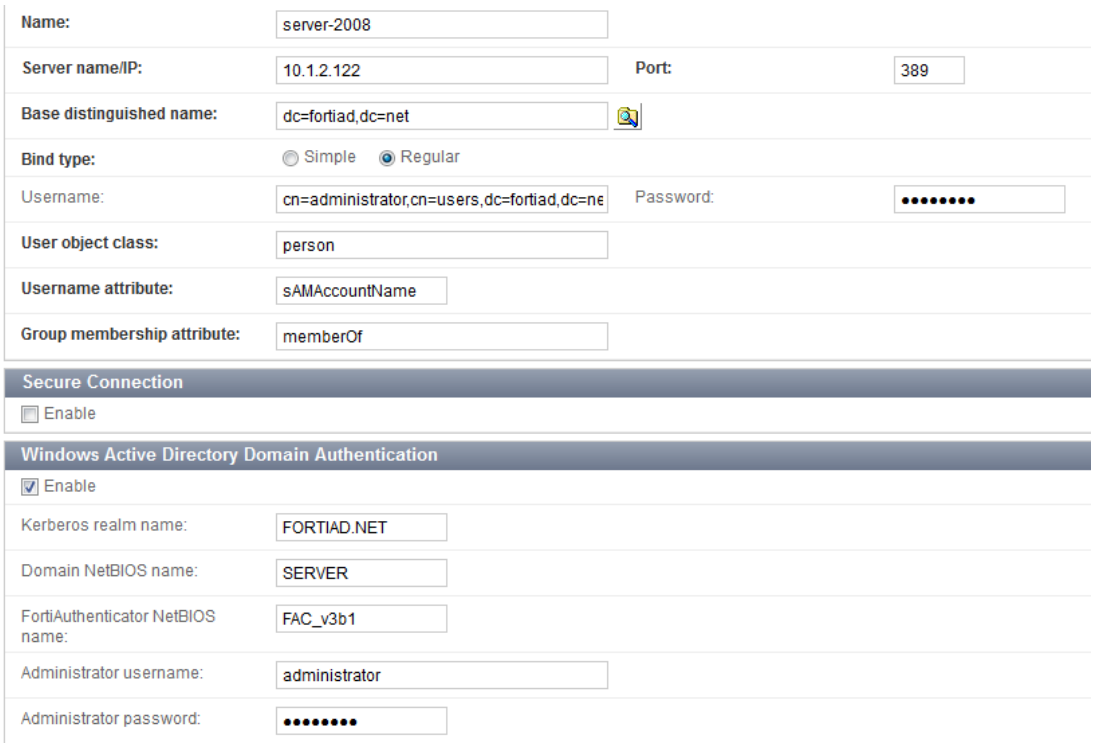
In the *Certificates* snap-in, open the *Personal* > *Certificates* folder. This is where you should find the imported certificate. If this is not the case, do not proceed until the certificate is in place.



This completes the Windows management console tasks, feel free to close the mmc or save the view, it is no longer required in this setup. The certificate tasks on the FortiAuthenticator are now also complete.

FortiAuthenticator Directory Services Configuration

The following section covers FortiAuthenticator directory integration. To configure integration with a remote AD/LDAP, within the user interface, under *Authentication* > *Remote Auth. Servers* > *LDAP*, click on *Create New*, and complete the AD server settings similar to the output below:



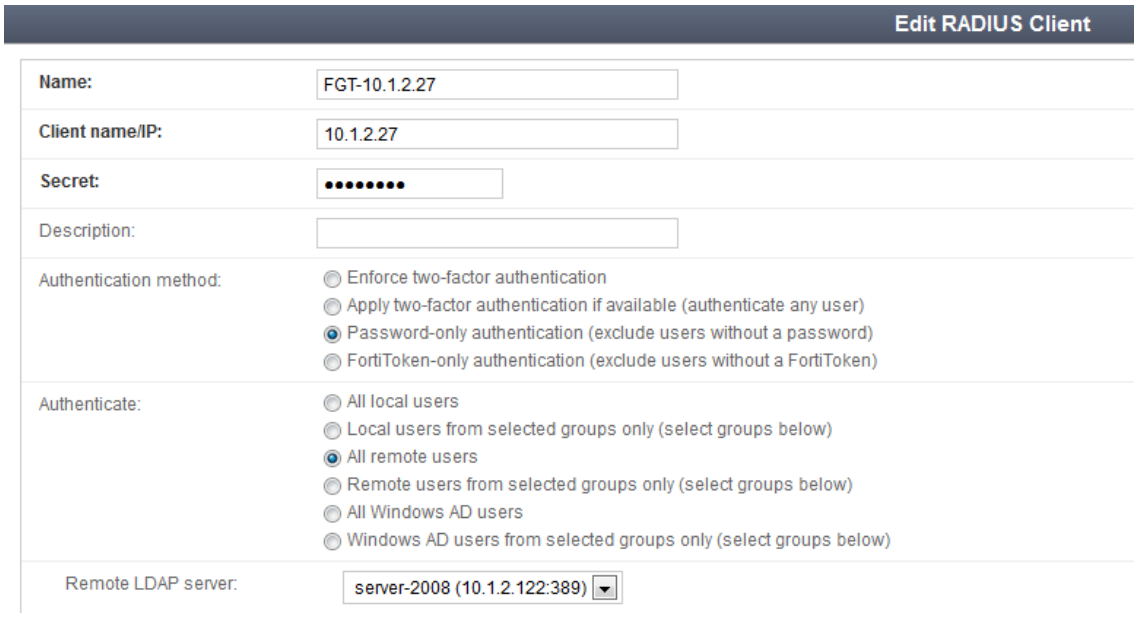
The username and password required do not necessarily have to belong to an administrator; the user only requires enough rights to browse the directory for the purposes of pulling users and groups into the FortiAuthenticator. The *Windows Active Directory Domain Authentication* section does not have to be completed as a requirement for this configuration.

Once the details have been entered, click on the folder icon (next to the *Base Distinguished Name* field) to ensure that you can browse the directory. If the directory is accessible, close the browsing window and click on *OK*.

The next step is to import the user (the one intended for SSL remote access) from the directory to the FortiAuthenticator. The user must be in place on the FortiAuthenticator as in the current version (v3.0), as unknown user authentication is not supported.

In the user interface go to *User Management* > *Remote Users* and click on *Import*, then select the relevant pre-defined remote LDAP server and click on *Import Users*. From the pop-up window select the relevant user(s) and click on *OK*. The remote user(s) should appear as follows:

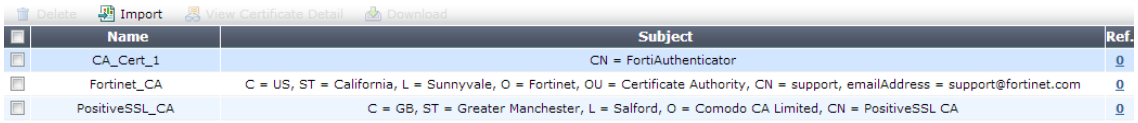
The final FortiAuthenticator task is to define the FortiGate as a RADIUS client. In the interface, go to *Authentication* > *RADIUS Service* > *Clients* and click on *Create New*. Then enter the appropriate details (example below) and click on *OK*.



FortiGate Certificate Configuration

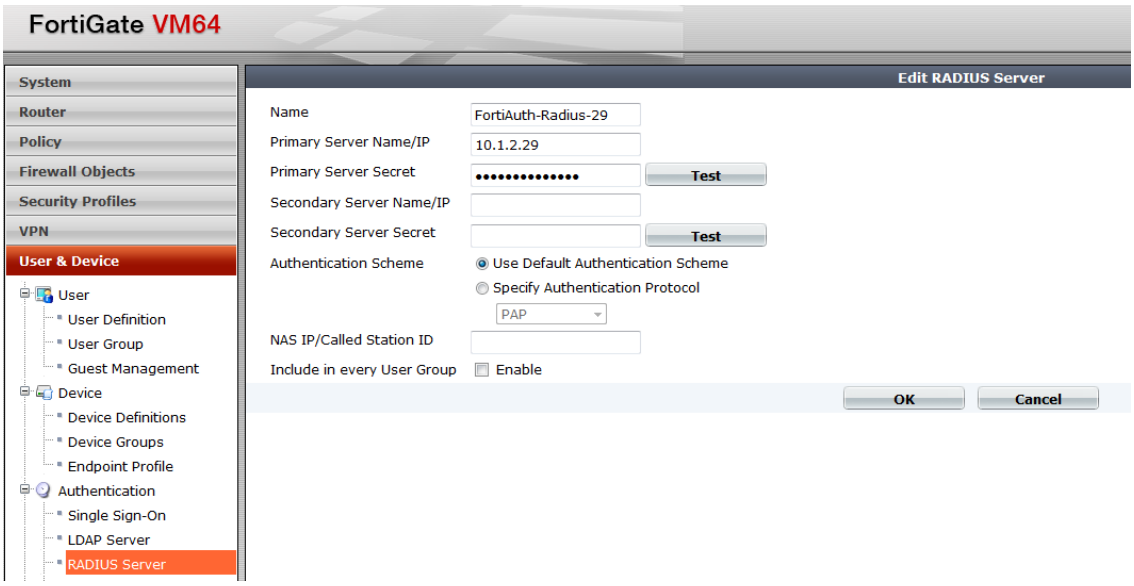
The next set of tasks will be carried out on the FortiGate. Initially the FortiAuthenticator root certificate needs to be imported into the FortiGate. To do this, within the user interface, go to *System* > *Certificates* > *CA Certificates* and then click on *Import*. Click *Local PC* and choose your file, then select the root certificate and click on *OK*.

The imported root CA should look as follows:

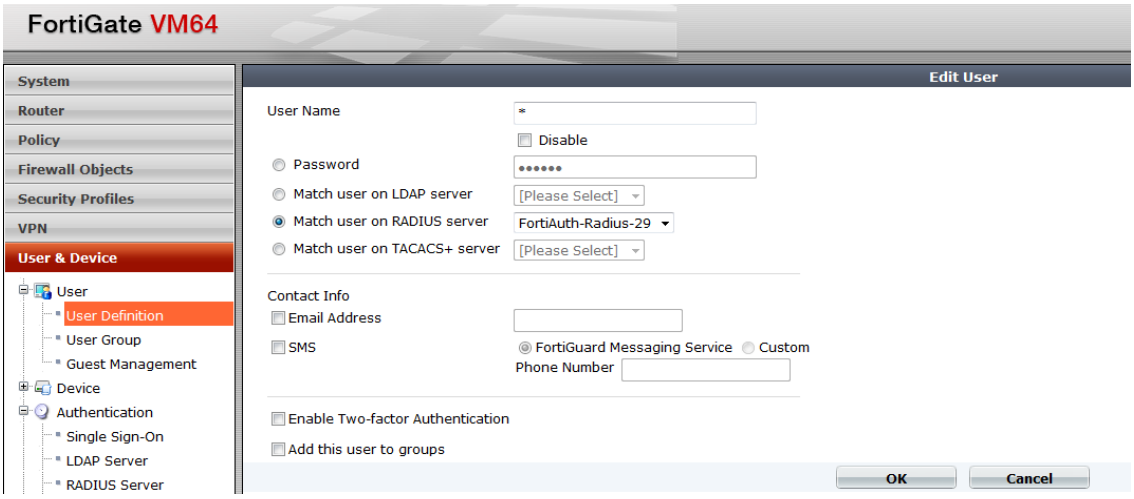


FortiGate RADIUS Client Configuration

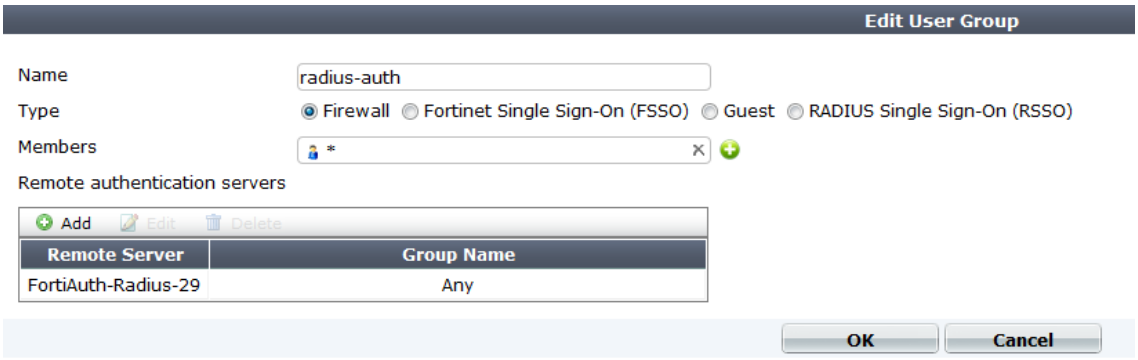
The FortiGate now needs to be configured as a RADIUS client to the FortiAuthenticator. Within the FortiGate interface, go to *User & Device* > *Authentication* > *RADIUS Server* and click on *Create New*. Complete the RADIUS server details, and then test the connection, example below:



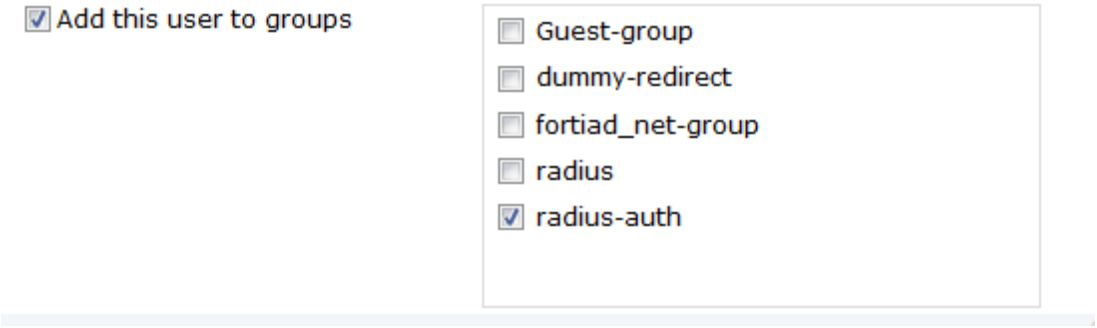
Next, a wildcard RADIUS user needs to be created. Go to *User & Device* > *User* > *User Definition* and click on *Create New*. Create a wildcard user as shown below. A wildcard user will allow the FortiGate to send all RADIUS authentication requests to the FortiAuthenticator.



The next RADIUS configuration step is to create the RADIUS group on the FortiGate which will host the user(s) for the SSL-VPN. Within the FortiGate go to *User & Device* > *User* > *User Group*, click on *Create New*, and create a firewall authentication group that includes the wildcard user and references the FortiAuthenticator, example below:

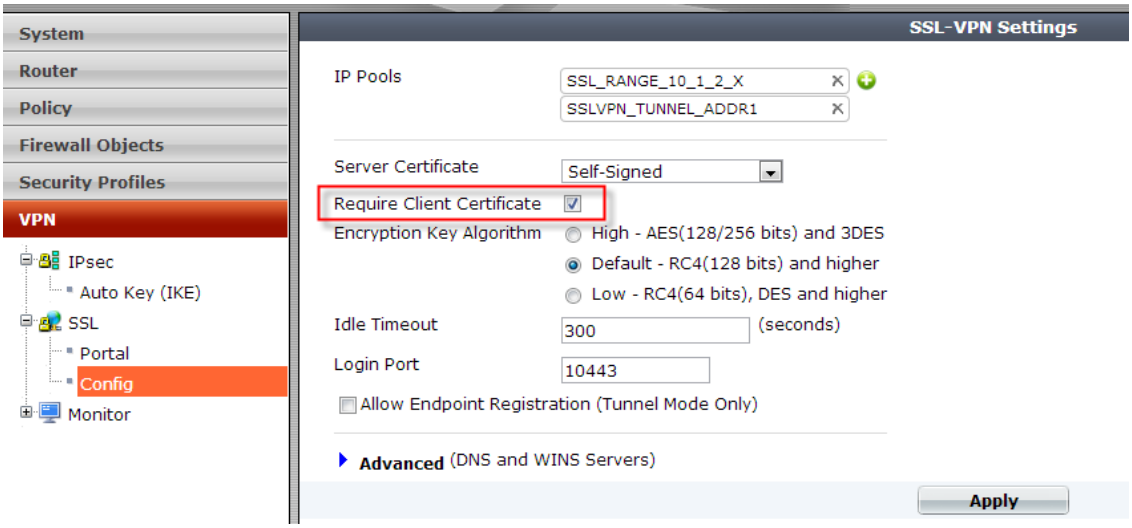


Go back to the wildcard user in *User & Device* > *User* > *User Definition* and add the wildcard user to the RADIUS group and *OK* the changes, example below:

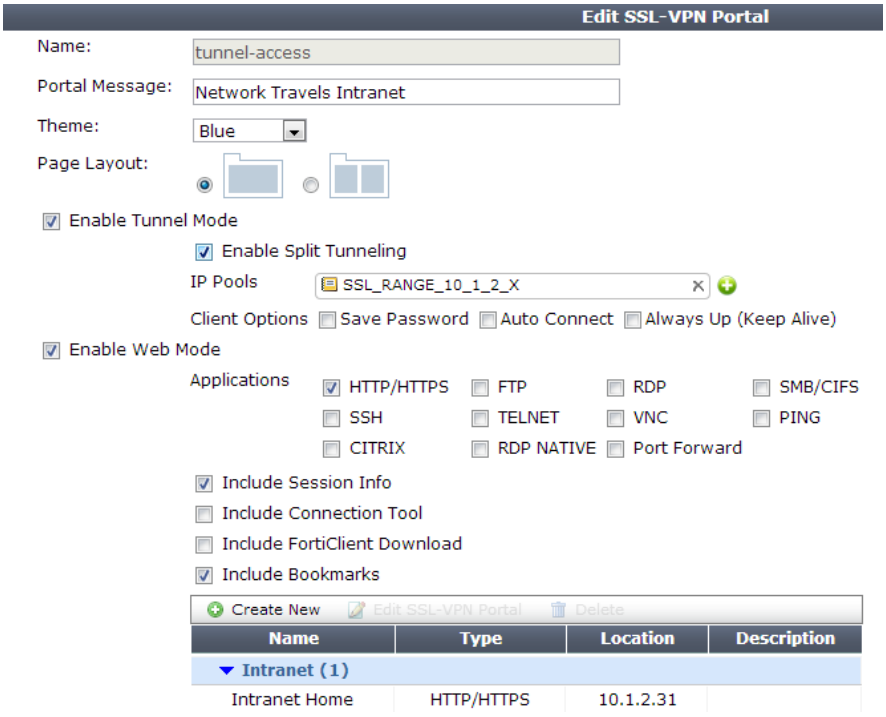


FortiGate SSL-VPN Configuration

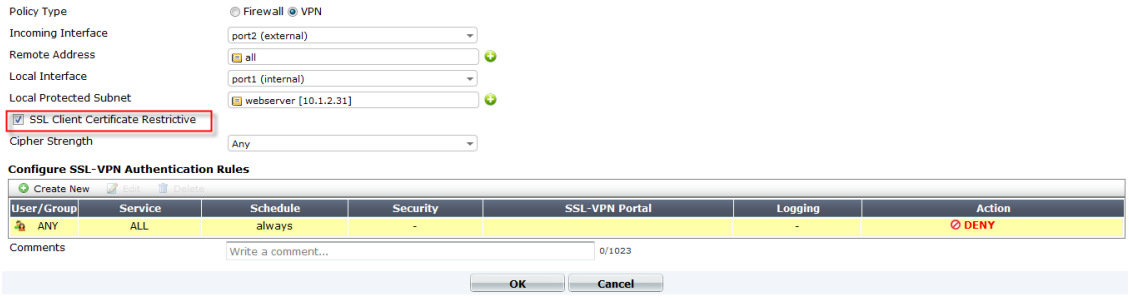
The following steps address SSL-VPN creation on the FortiGate. Firstly ensure that there is a valid IP pool in place (under *Firewall Objects* > *Addresses*), if using an IP tunnel based VPN. To begin the SSL configuration, for both IP tunnel based and browser only VPN, go to *VPN* > *SSL* > *Config* and ensure the relevant settings are in place. Also make sure that the *Require Client Certificate* tickbox is selected, as in the example below:



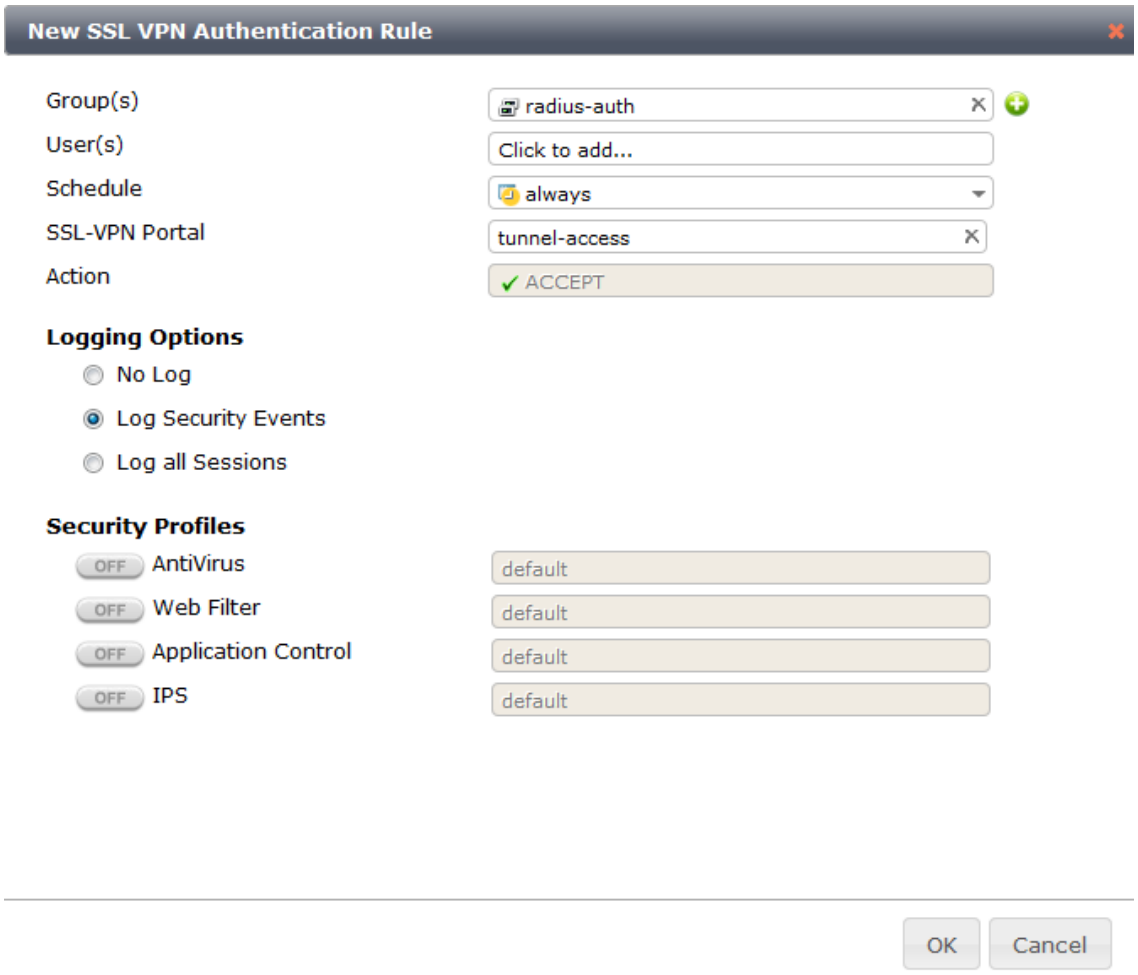
Under *VPN* > *SSL* > *Portal* create the relevant SSL portal interface based on your VPN type (either IP tunnel or browser only). IP tunnel based VPN is shown in the example below:



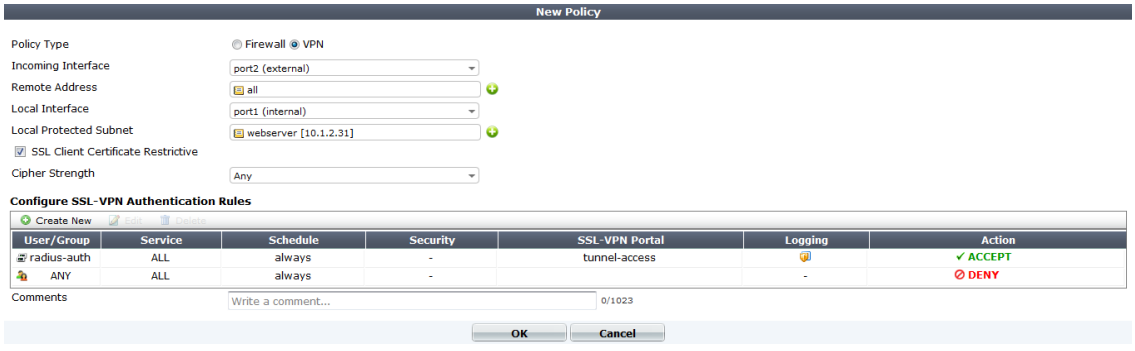
Within the FortiGate, go to *Policy & Objects* > *IPv4*, click on *Create New*, then click on VPN setup and create an external interface to internal interface SSL-VPN policy, ensuring that you enable the *SSL client restrictive* tickbox as shown in the example below:



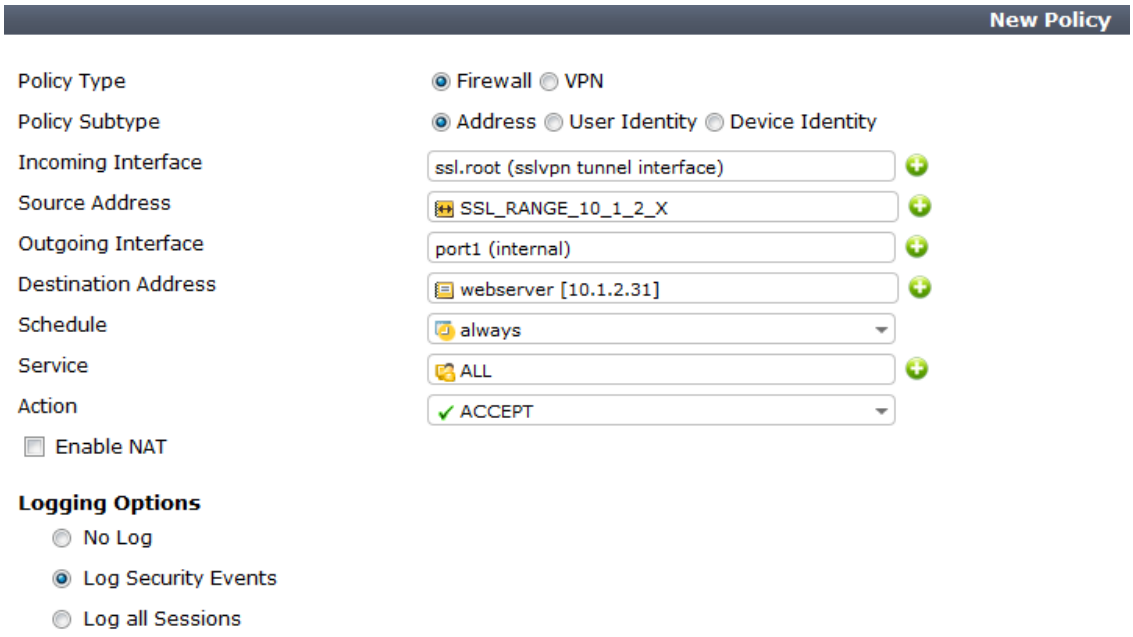
From within the policy configuration click on *Create New* under the *Configure SSL-VPN Authentication Rules* section and use the preconfigured RADIUS group and the SSL-VPN portal as in the example below. *OK* the changes and then *OK* the main policy.



If the completed SSL policy is selected and edited, the configuration should be as follows:



When configuring an IP tunnel SSL-VPN (using the FortiClient), an additional firewall policy is required (configured under *Policy & Objects* > *IPv4* and then *Create New*). This is to allow incoming connections from the SSL tunnel interface to the internal network. An example of this is as follows:

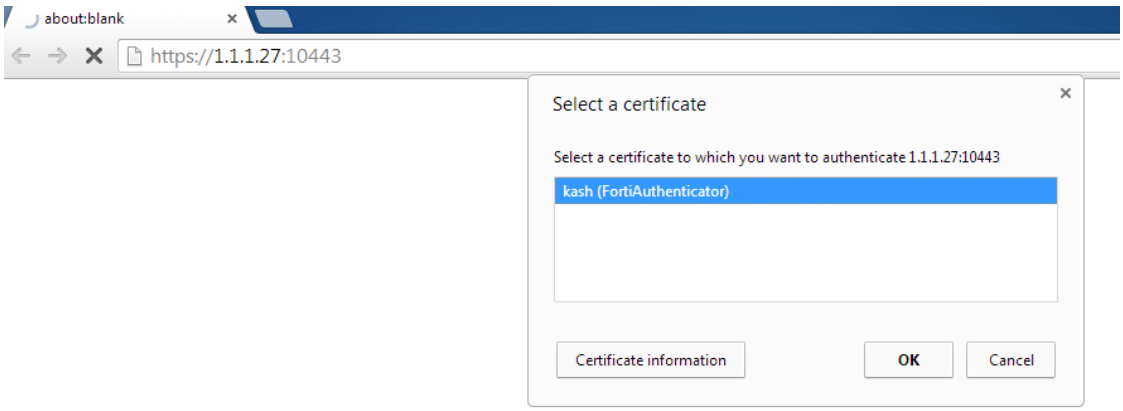


Once you *OK* the changes, the completed rule should look as follows in the policy section:

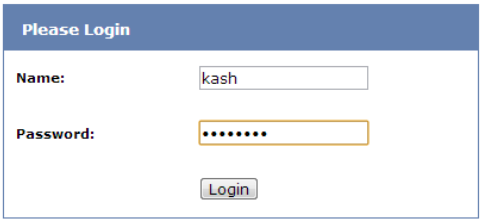
This completes all configuration steps. It is now time to test the VPN.

Testing, Logging and Monitoring

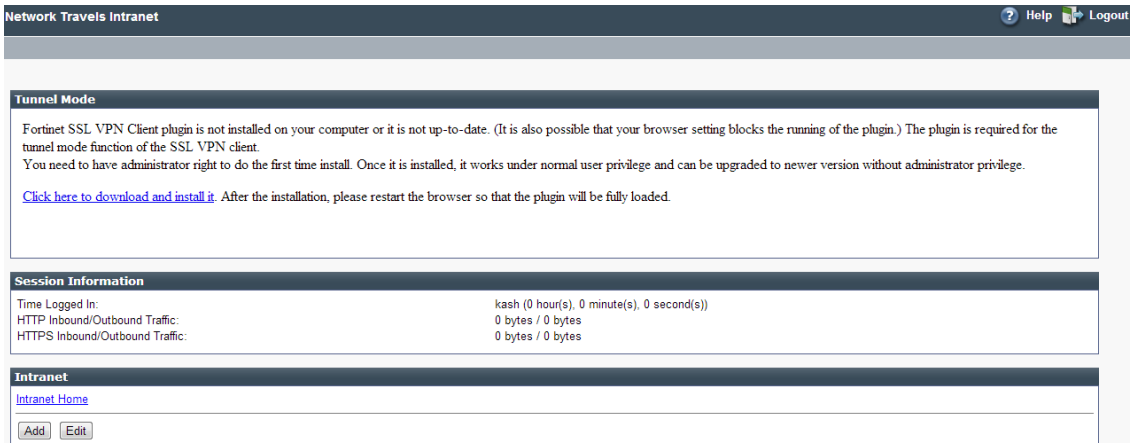
If the configuration is for a browser only SSL-VPN, then open a browser to the SSL-VPN gateway. Upon connecting to the gateway, the certificate negotiations should begin and the browser should prompt for a valid user certificate to be used for the VPN. Any certificates in the personal certificate store will be listed. See the example below using the Chrome browser:



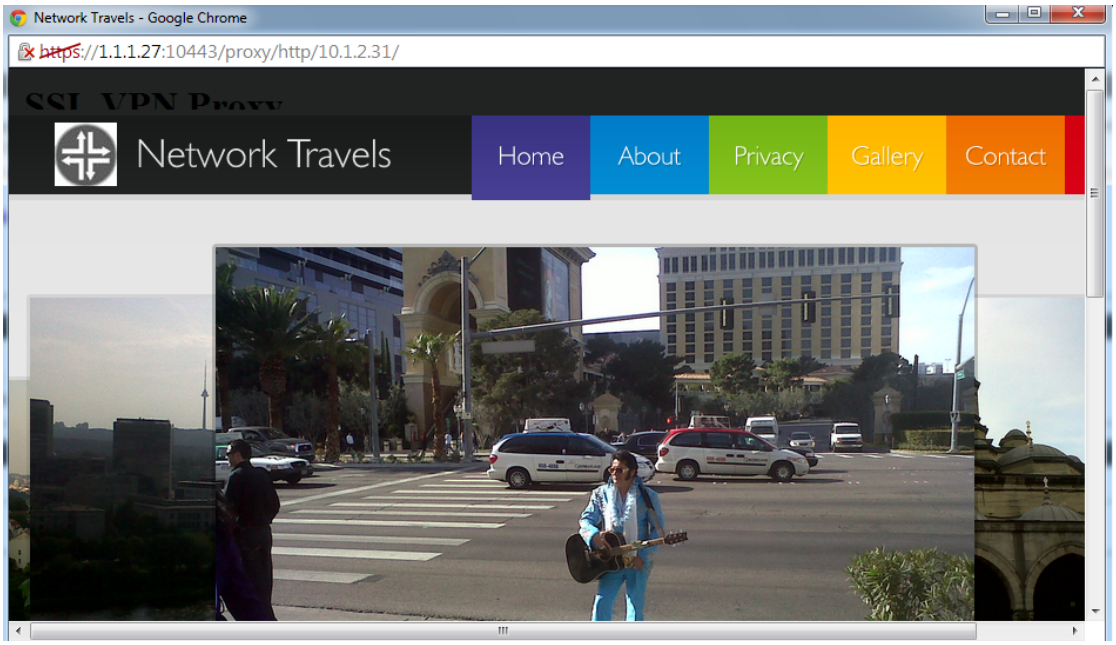
Upon successful certificate negotiations, a username and password prompt should appear. Even if the certificate negotiations fail, the username and password prompt will still appear, however it will not be possible to successfully authenticate, even if the username and password are valid.



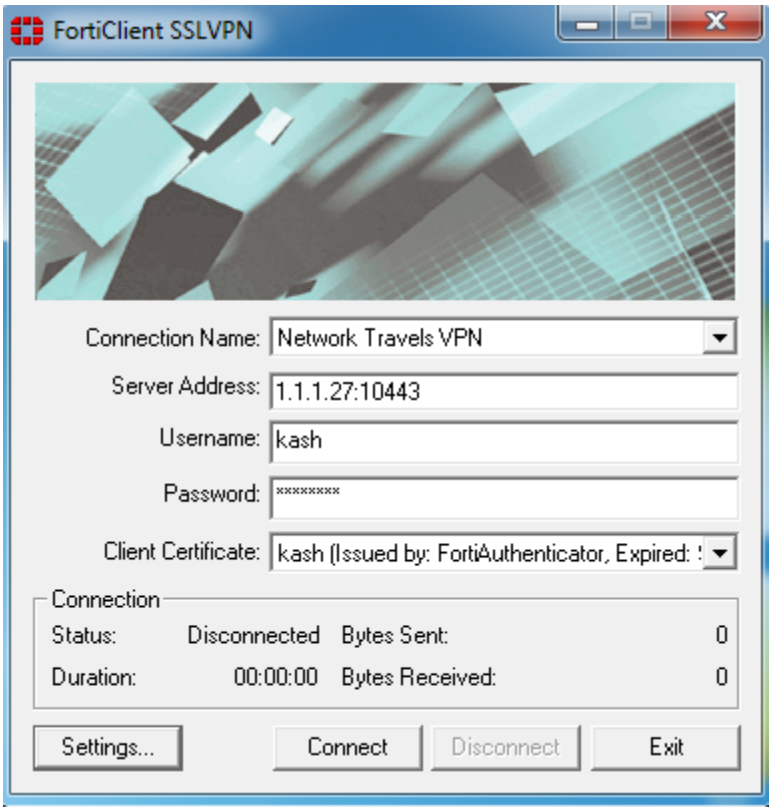
Once the current directory username and password have been entered, the SSL-VPN portal should be available. The example below is of the portal configured earlier in this guide:



Upon clicking on the Intranet homepage, the browser connection is then proxied to the internal web server, as shown in the example below:

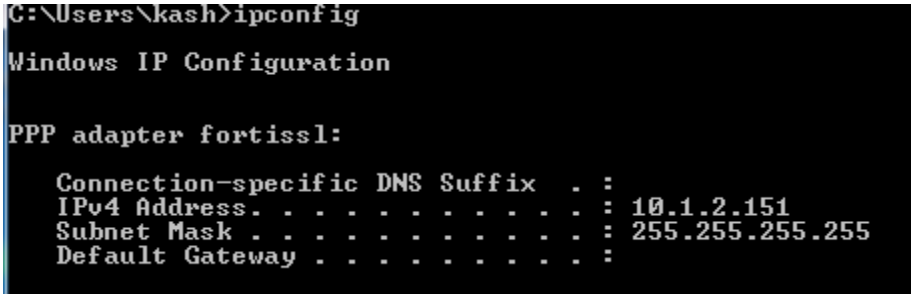


If the configuration is based on an IP tunnel configuration, then the FortiClient is required to initiate the connection. The FortiClient should automatically pull the personal certificate from the local certificate store and make it available in the connection settings. See the example below:

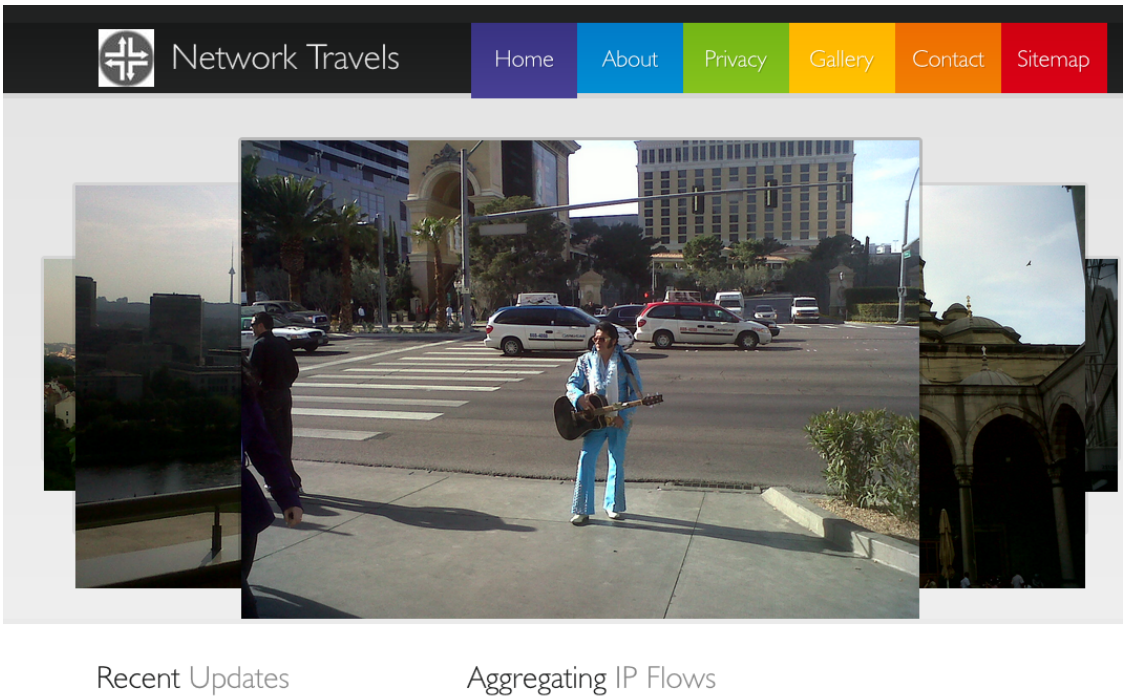


Click on *Connect* to initiate the VPN and certificate negotiations. If the certificate negotiations fail, there should be an *-12 error message* prompt and the VPN will not complete. If the certificate settings are valid and the

directory username and password are correct, the VPN should connect and data transfer should begin. To confirm that the client is connected, click on the Windows icon and enter *ipconfig*. The fortissl adapter should be visible with the correct preconfigured address.

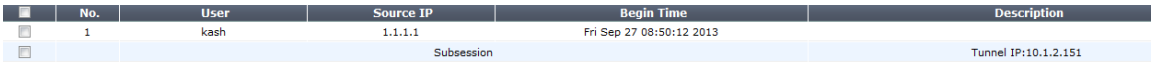


The client PC should be able to connect to the internal network directly; the image below is of the client browser connecting directly (via the 10.1.2.31 address) to the intranet.



If logging had been enabled on the relevant FortiGate firewall policies, these should also be incrementing their counters and indicating data transfer.

Within the FortiGate, under *VPN* > *Monitor* > *SSL-VPN Monitor*, the monitor status should indicate that the client is connected. In the example below, the tunnel IP is also shown as this is a IP tunnel based VPN.



	No.	User	Source IP	Begin Time	Description
	1	kash	1.1.1.1	Fri Sep 27 08:50:12 2013	
			Subsession		Tunnel IP:10.1.2.151

Within the FortiAuthenticator, under *Logging* > *Log Access* > *Logs*, the following entry confirms that the user has successfully authenticated against Active Directory.

386	Fri Sep 27 08:49:49 2013	information	Event	Authentication	20001	10.1.2.27	Remote LDAP user authentication with no token successful	kash

This completes and confirms the SSL-VPN client testing.

Additional Considerations - Certificate Checking

With the above setup, the FortiGate does not check the validity of the received client certificate. This can be achieved through the use of a CRL (Certificate Revocation List) and CDP (CRL Distribution Point). The CRL is a list of certificates the FortiAuthenticator has revoked, and is available to download as a static list. The CDP is in every certificate the FortiAuthenticator issues and provides a link for the CRL. OCSP (Online Certificate Status Protocol) is a real-time certificate check with the Certificate Authority. Upon receipt of a certificate, a device can check the validity of the certificate from the issuing authority by using OCSP. FortiAuthenticator supports CRLs, CDPs and OCSP.

The dynamic OCSP CRL is accessible via the URL:

http://<FortiAuthenticator_IP>:2560

Added Benefits

- FortiAuthenticator can introduce Certificate Management to an existing FortiGate install base with minimal disruption.
  - With an easy to use interface and rich feature set, customers can increase the security of existing SSL or IPSec VPNs.
- FortiAuthenticator supports SCEP (Simple Certificate Enrolment Protocol), which means users can generate and auto-enroll their certificates, rather than manually creating them.
- Very useful in BYOD and smartphone/tablet scenario's.
- FortiAuthenticator can import users from an existing directory server and associate multiple authentication methods to the user such as FortiTokens, SMS and E-mail.
- Users and Groups can be auto-imported (based on rules) from the directory server.
- Active Directory authenticated users can feed into the FSSO (Fortinet Single Sign-On) framework allowing Identity Based access control across the network.